

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

ME/2171
#2

In re application of: **Brown et al.**

Serial No.: **09/884,490**

Filed: **June 18, 2001**

For: **Method and Apparatus for
Removing Information from a Server**

35525

PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

§
§
§
§
§
§
§

Group Art Unit: **2171**

Examiner: **Amsbury, Wayne P.**

Attorney Docket No.: **AUS920010546US1**

Certificate of Mailing Under 37 C.F.R. § 1.8(a)

I hereby certify this correspondence is being deposited with the United States Postal Service as First Class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on April 26, 2004.

By: Michele Morrow
Michele Morrow

TRANSMITTAL DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RECEIVED

MAY 06 2004

Technology Center 2100

Sir:

ENCLOSED HERewith:

- Appellant's Brief (in triplicate) (37 C.F.R. 1.192); and
- Our return postcard.

A fee of \$330.00 is required for filing an Appellant's Brief. Please charge this fee to IBM Corporation Deposit Account No. 09-0447. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0447. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0447.

Respectfully submitted,

Duke W. Yee
Duke W. Yee
Registration No. 34,285
YEE & ASSOCIATES, P.C.
P.O. Box 802333
Dallas, Texas 75380
(972) 367-2001
ATTORNEY FOR APPLICANTS



#12

Docket No. AUS920010546US1

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Brown et al.**Serial No. **09/884,490**Filed: **June 18, 2001**For: **Method and Apparatus for
Removing Information from a Server**§
§
§
§
§
§
§Group Art Unit: **2171**Examiner: **Amsbury, Wayne P.**

RECEIVED

MAY 06 2004

Technology Center 2100

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450ATTENTION: Board of Patent Appeals
and InterferencesCertificate of Mailing Under 37 C.F.R. § 1.8(a)I hereby certify this correspondence is being deposited with the
United States Postal Service as First Class mail in an envelope
addressed to: Commissioner for Patents, P.O. Box 1450,
Alexandria, VA 22313-1450 on April 26, 2004.

By:

Michele Morrow
Michele Morrow

APPELLANT'S BRIEF (37 C.F.R. 1.192)

This brief is in furtherance of the Notice of Appeal, filed in this case on February 25, 2004.

The fees required under § 1.17(c), and any required petition for extension of time for filing this
brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL
BRIEF.

This brief is transmitted in triplicate. (37 C.F.R. 1.192(a))



REAL PARTIES IN INTEREST

RECEIVE

MAY 06 2004

Technology Center 21

The real party in interest in this appeal is the following party: International Business Machines Corporation.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-34

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: NONE
2. Claims withdrawn from consideration but not canceled: NONE
3. Claims pending: 1-34
4. Claims allowed: NONE
5. Claims rejected: 1-34

C. CLAIMS ON APPEAL

The claims on appeal are: 1-34

STATUS OF AMENDMENTS

There are no amendments after final rejection.

SUMMARY OF INVENTION

The present invention provides for a method and apparatus for managing confidential information in a data processing system server. See page 13, lines 29-32. Information is received from a plurality of users. See page 13, line 32 to page 14, line 2. The information is stored on a server for many different uses and in many different files and databases. See page 13, lines 10-28. A request is received from the client to remove specific selected information from the stored information for a user within the set of users, wherein the selected information is received in response to a transaction involving that user. See page 14, lines 2-11. In response to receiving the request, the selected information is removed from the stored information, thus maintaining the privacy requests of that user. See page 14, lines 11-18.

ISSUES

The only issue on appeal is whether claims 1-34 are anticipated under 35 U.S.C. § 102(e) based on Cooper et al. (US 2001/0051996 A1).

GROUPING OF CLAIMS

The claims do not stand or fall together. The claims stand or fall in accordance with the following grouping of claims, the reasons for the groupings being provided in the argument section below:

- Group I - claims 1, 4-6, 11, 12, 14, 17-19, 24, 28 and 32;
- Group II - claims 2 and 15;
- Group III - claims 3 and 16;

- Group IV - claims 7 and 20;
- Group V - claims 8-10, 13, 21-23, 25, 26, 30 and 34; and
- Group VI - claims 27, 29, 31 and 33.

ARGUMENT

The Final Office Action rejects claims 1-34 under 35 U.S.C. § 102(e) as being anticipated by Cooper et al. (US 2001/0051996 A1). The rejection is respectfully traversed.

Cooper is directed to a method for transferring electronic media information over a public network in such a way as to provide safeguards for inappropriate distribution of copyright or otherwise protected materials. The media information is transparently watermarked with a unique ID, such as one generated from X.509 Digital Certificate and public-key cryptography public/private key pairs, such that the information can be identified as belonging to a particular individual. Cooper also provides a method for monitoring the movement of such watermarked files, positively identifying people who have inappropriately distributed copyright materials over a public network without permission, and taking appropriate enforcement action against such people.

Appellants respectfully submits that, contrary to the allegations made in the Final Office Action, the Cooper reference does not, in fact, teach receiving a request to remove selected information from the stored information from a user within the set of users, wherein the selected information is received in response to a transaction involving the user, as recited in independent claims 1, 11, 12, 14 and 24.

Claim 1, which is representative of the other rejected independent claims 11, 12, 14 and 24, reads as follows:

1. A method in a data processing system for managing information, the method comprising:
 - receiving information from a plurality of users;
 - storing the information to form stored information;
 - receiving a request to remove selected information from the stored information from a user within the set of users, wherein the selected information is received in response to a transaction involving the user; and
 - responsive to receiving the request, removing the selected information from the stored information.

Appellants respectfully submit that Cooper does not teach receiving a request to remove selected

information from the stored information from a user within the set of users, wherein the selected information is received in response to a transaction involving the user. Furthermore, Appellants respectfully submit that the Cooper reference does not teach removing the selected information from the stored information responsive to receiving the request.

In response to the argument that Cooper does not teach receiving a request to remove selected information from the stored information from a user within the set of users, wherein the selected information is received in response to a transaction involving the user, the Final Office Action, on page 2, states:

In the Telephone interview of 10/17/03 and in the Response, Applicants attempt to draw distinction between revoke and remove. Firstly, there is no evidence in the Disclosure that the removal of data from memory means anything other than the usual removal of access, which would allow garbage collection processes to reclaim the memory space. Secondly, Webster's New Riverside University Dictionary, Houghton Mifflin Company, ©1984, 1988, defines revoke as meaning to nullify by withdrawing, recalling or reversing. There is no obligation of the revoking authority to re-instate, and thus revocation is equivalent to removal.

Applicants correctly states that patentability depends on each and every element of a claim, but then argues claims 2-7 in terms of element 2, whereas claims 3-7 depend directly on claim 1 and do not include that element. (The arguments concerning claims 8-26 are included in this analysis.) New claims 27-34 are addresses below.

As to claim 1, Applicant states [page 11] that Cooper does not teach receiving a request to remove selected information, received from a user in response to a transaction involving the user. To reiterate the rejection, Cooper is directed to transactions in which a user, who obtains a digital certificate which allows access to content selected by the user. [See also 0018; 0060 lines 6-9.] Of course this is done by some management system, but so are the steps of the claims, and a user request is required to trigger the process. As noted at [0065], any entity may act as the certification authority that revokes a user's digital certificate [0069]. Again, such an act cannot be arbitrary, but inherently must be initiated by request, which is itself a transaction in the system.

Appellants respectfully disagree that Appellants' disclosure contains no evidence that the removal of data from memory means anything other than the usual removal of access. To the contrary, throughout the present description it is stated that the present invention's whole intent is to provide a user with the ability to "remove" their personal or confidential information from a server. For example, this is referred to on page 4, lines 12-18; page 12, lines 25-28; page 20, lines 7-10 and elsewhere.

One example section of the present specification that provides support for removal of selected information is found on page 14, lines 6-18, of the specification, which reads as follows:

A user may identify personal or confidential information sent to server 400 through security process 414. A request may be generated and sent to server 400 to remove this information. The request is received by Web server 406 and sent to security process 412 for handling. If the information is no longer required for a particular transaction, security process 412 removes the information from client information database 410. A confirmation is then returned to the user at client 402, indicating that the information has been removed. If the information is still required for the transaction, such a notice is returned to the user.

This section of Appellants' specification provides adequate disclosure that a user identifies personal or confidential information that is intended for removal, a request is received to remove the information and, if the information is no longer required, the information is removed from the client information database. The whole reason for the present invention is to remove information from a server so that it is no longer accessible by the server. This is clear from the many sections of the disclosure referenced above and many other portions of the disclosure that are not explicitly pointed to above. Simply "revoking" information does not achieve this purpose.

In determining the scope of a term in the claims, the Examiner must look to both the intrinsic evidence provided in the disclosure and may, when the intrinsic evidence is considered not sufficient, consider extrinsic evidence provided by other sources. As discussed above, the intrinsic evidence provided when reading the claims in view of the specification makes it clear that the term "remove" means to completely delete or "get rid of" the information so that it is no longer accessible in the stored information. This is clear from page 20, lines 7-10, which state that the particular mechanism of the present invention is used for "removing traces of personal or confidential information, such as a credit card number or a social security number." Removing traces of personal or confidential information means to completely remove or delete this information so that it is not accessible by the server. Simply "revoking" information would not remove all traces of personal or confidential information. In fact, "revoking" leaves the information but revokes the ability to use the information. Thus, traces of the personal or confidential information are still present when the information is simply "revoked."

Furthermore, other sections of the specification make it clear that there is complete removal so that there is no accessibility to the information is intended by the term "remove." For example, Figure 11 and page 19, lines 14-17 state that "removal of the confidential information from the database may not occur if the confidential information is still required for the transaction." It is clear from this statement that if the information is removed, the server would not be able to complete the transaction because the information is no longer present. If the information were simply "revoked", the transaction could complete and then the information not be used again but still be present in the server. Again "removal" is not the same as "revoking."

Thus, the intrinsic evidence found within the disclosure clearly points to the term "remove" meaning to completely remove or delete so that the information is no longer present in the stored information. Moreover, Appellants' own arguments have limited the definition of the term "remove" to have this definition and to not include simply "revoking" the information. Therefore, the Examiner should interpret the term "remove" in the manner asserted by Appellants.

However, if the intrinsic evidence and Appellants' arguments are not considered to be sufficient, the extrinsic evidence also points to the term "remove" being different and not synonymous with "revoke." The term "remove" is defined by Webster's Dictionary, Random House Inc., ©1996, 1993 as meaning "to do away with" or "eliminate." The Examiner's provided definition of "revoke" is contrary to the definition of "remove." The Examiner states that the definition of the term "revoke" is "to nullify by withdrawing, recalling or reversing" as per Webster's New Riverside University Dictionary, Houghton Mifflin Company, ©1984, 1988. It is conspicuous that the Examiner's own definition of "revoke" does not mention "removing" and the term "remove" is not identified by Webster's as a synonym of "revoke." This is because "nullifying" is not the same as "removing." The term "nullify" means to invalidate, not to completely remove or delete so that there is no trace of the information left, as with the term "remove." Furthermore, Appellants respectfully submit that neither "revoke" nor "remove" are synonyms of each other as per Roget's II, The New Thesaurus, Houghton Mifflin Company, © 1980.

Moreover, Appellants respectfully disagree with the Examiner's statement that "There is no obligation of the revoking authority to re-instate, and thus revocation is equivalent to removal." Nowhere in Cooper is it taught that revocation of a user's digital certificate is equivalent to removal. To the contrary, Cooper teaches that the digital certificate must be retained for further investigation at paragraph [0148], which reads as follows:

[0148] For this reason, other security precautions may be taken. The CPS may additionally contain a password that must be correctly matched by the legitimate consumer at the time the hardware device containing the digital certificate logs on to the VPN. If an attempt to enter the password fails more than a predetermined number of times, the digital certificate may be immediately revoked by the Authenticate User and Get Digital Certificate step 320 until a further investigation may be conducted. (emphasis added)

This section of Cooper teaches that if an invalid password is entered too many times the digital certificate is revoked until a further investigation may be conducted. If Cooper were to teach as the Examiner alleges, "revocation is equivalent to removal," then Cooper would not be able to investigate the invalid use of the password tied to the digital certificate as it would no longer exist. Thus, Cooper does not teach removal of client information from the client information database in response to a request from a user, which identifies personal or confidential information that is intended for removal.

Still further, the revocation of the digital certificate as taught by Cooper is in response to an invalid password being entered is not a request from a user to remove selected information from the stored information of a user in response to a transaction involving the user. The revocation of the digital certificate is not an intended request to remove information about the user. Additionally, as shown above, if the entry of an invalid password were intended to remove information about the user, the teachings of Cooper would not perform the desired function. That is, the use of an invalid password by the user would result in the user no longer being able to access the information, but the information about the user is still in the stored information of the Cooper system.

Thus, in view of the above, Appellants respectfully submit that Cooper does not teach each and every feature of independent claims 1, 11, 12, 14 and 24 as is required under 35 U.S.C. § 102(e). At least by virtue of their dependency on claims 1 and 14, Cooper does not teach each and every feature of dependent claims 4-6, 17-19, 28 and 32. Accordingly, Appellants

respectfully submit that the rejection of claims 1, 4-6, 11, 12, 14, 17-19, 24, 28 and 32 under 35 U.S.C. § 102(e) should be overturned.

Additionally, in regard to dependent claim 2, Cooper does not teach determining whether the request is a valid request and preventing removing of the selected information in response to a determination that the request is an invalid request. The Examiner states the following:

The digital identification of a user or owner is a "consumer ID" is used to verify any message from a user [0042]. Alternatively, a digital certificate may be checked to see if it is valid or invalid [0124].

Paragraph [0042] in Cooper reads as follows:

[0042] As used herein, the term "consumer ID" refers to a positive digital identification of the user, computer, or player device owned by a person who downloads content, has access to content download systems, or can access the systems described in this patent. A positive digital identification may be any one or a plurality of the following: an individual's digital certificate, a digital certificate or digital certificate serial number digitally signed using the user's private key, a transactional ID digitally signed using a user's private key that can be verified via the user's public key, the serial numbers of computers or player devices owned by or registered to a user, a message received by a system containing verified biometrics data (fingerprint, face recognition, eye/retina recognition, voice recognition etc.), or other legally recognizable means to identify an individual.

This section teaches that a Consumer ID is used as identification means for a use, computer or player device. Paragraph [0124] in Cooper reads as follows:

[0124] With a Content Registry system 234, a player of content may check the registry to see if an identical digital certificate is being played by another player device. This may be achieved by communicating with the Copyright Registry 234 on-line using a network 116, for example the Internet, an Intranet, or other network. Certain in-use switches may be set to indicate that a user is currently using a particular content file. Following is an example of this. A software program that has been previously registered with the Copyright Registry 234 is initiated by an end user. During the program initialization process, the Copyright Registry 234 is checked to see if someone else is using the same software program with the same digital certificate. If so, then piracy has been detected and the author or publisher may decide how best to communicate an appropriate message to the parties using the software. If a no match condition is found, the content file plays normally. When the content file reaches its end, then the Copyright Registry 234 may be updated to indicate that the content file and the digital certificate for that content file are no longer being played. An in-use switch

will be set back to False, Null, Zero, or other value that indicates the content is no longer being played.

This cited section teaches authenticating digital certificates to see if an identical certificate is being used elsewhere and thus detecting piracy. If piracy is detected, a message is sent to the author or publisher for appropriate action. While these sections of Cooper teach a Consumer ID and authentication, they do not teach preventing removal of information in response to the request being invalid. Furthermore, the authentication of the digital certificate in these sections do not have anything to do with "revoking a user's digital certificate," in paragraph [0069], which is part of a set of operations that may be performed by a certificate authority.

Claim 3 recites that at least one of a certificate, a password, and a key is used to determine whether the request, which is a request to remove selected information from the stored information from a user within the set of users, is valid. As shown above, Cooper teaches away from removing information about a user and instead revokes the user's access to the information. Thus, Cooper does not teach validating a request to remove selected information from stored information based on at least one of a certificate, a password, and a key.

Claim 7 recites the request sent to the user is in a form of an applet requesting personal information about the user. The Examiner stated in the previous Office Action dated July 11, 2003 that "Cooper is intended to be used with the Internet, which typically applies applets within the Java language." Simply using the Cooper system with the Internet does not necessitate the use of applets. There are many server functions that are performed without using applets. For example, scripts, HTML based forms, or a plurality of other tools may be used. Thus, simply stating that the Cooper system is "intended to be used with the Internet" does not sufficiently address the feature of an applet being used to request personal information about a user.

Furthermore, as stated in the previous Response, the Examiner fails to address the specific features of claims 8-13, 21-23 and 25-26, and merely alleges, without any supported evidence, that these claims are rejected on the same basis as claims 1-7, even though they contain additional features. For example, claim 8 contains the feature of sending a Web page to a user at a client. Nowhere in the Final Office Action or the Office Action dated July 7, 2003, does the Examiner provide a specific section of the Cooper reference that teaches this feature. The Office

Action simply fails to establish a prima facie case of anticipation for claims 8-13, 21-23, 25 and 26.

Additionally, the Final Office Action alleges that the feature of the request to remove selected information originates from a client device of the user, as recited in claims 27, 29, 31 and 33, and is taught at paragraph [0058] and [0065]. As shown above, Cooper does not teach receiving a request to remove selected information from the stored information from a user within the set of users and instead revokes the user's access to the system in response to a user inputting the wrong password. As to dependent claims 28, 30, 32 and 34, these claims are dependent on independent claims 1, 8, 14 and 21, respectively, and overcome Cooper for the reasons shown above.

Furthermore, Cooper does not provide any teaching, suggestion, or incentive to make the needed changes to reach the presently claimed invention. Cooper actually teaches away from the presently claimed invention because this cited reference teaches retaining all information regarding the user and simply revoking access to the information, as opposed to receiving a request to remove selected information from the stored information from a user within the set of users, where the selected information is received in response to a transaction involving the user and responsive to receiving the request, and removing the selected information from the stored information, as in the presently claimed invention. Absent the Examiner pointing out some teaching or incentive to implement Cooper to receive a request to remove selected information from the stored information from a user within the set of users, where the selected information is received in response to a transaction involving the user and responsive to receiving the request, removing the selected information from the stored information as in the presently claimed invention, one of ordinary skill in the art would not be led to modify Cooper to reach the present invention when the reference is examined as a whole. Absent some teaching, suggestion, or incentive to modify Cooper in this manner, the presently claimed invention can be reached only through an improper use of hindsight using the Applicants' disclosure as a template to make the necessary changes to reach the claimed invention.

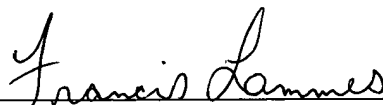
Thus, in view of the above, Applicants respectfully submit that Cooper does not teach each and every feature of independent claims 1, 8, 11-14, 21, 24 and 25 as required under 35 U.S.C. § 102(e). At least by virtue of their dependency on claims 1, 8, 14, 21 and 25,

respectively, Cooper does not teach each and every feature of dependent claims 2-7, 9, 10, 15-20, 22, 23 and 16-34. Accordingly, Appellants respectfully submit that the rejection of claims 1-34 under 35 U.S.C. § 102(e) should be overturned.

CONCLUSION

In view of the above, Appellants respectfully submit that claims 1-34 are allowable over the cited prior art and that the application is in condition for allowance. Accordingly, Appellant respectfully requests that the Board of Patent Appeals and Interferences not sustain the rejections set forth in the Final Office Action.

Respectfully submitted,

A handwritten signature in cursive script, reading "Francis Lammes", written over a horizontal line.

Francis Lammes
Reg. No. 55,353
Yee & Associates, P.C.
PO Box 802333
Dallas, TX 75380
(972) 367-2001

APPENDIX OF CLAIMS

The text of the claims involved in the appeal are:

1. A method in a data processing system for managing information, the method comprising:
receiving information from a plurality of users;
storing the information to form stored information;
receiving a request to remove selected information from the stored information from a user within the set of users, wherein the selected information is received in response to a transaction involving the user; and
responsive to receiving the request, removing the selected information from the stored information.
2. The method of claim 1, wherein the step of receiving a request includes:
determining whether the request is a valid request; and
preventing removing of the selected information in response to a determination that the request is an invalid request.
3. The method of claim 1, wherein at least one of a certificate, a password, and a key is used to determine whether the request is valid.
4. The method of claim 1, wherein the selected information is personal information about the user.

5. The method of claim 4, wherein the personal information includes at least one of a user name, a user identification, a password, a telephone number, an e-mail address, a physical address, a social security number, a birth date, and a credit card number.
6. The method of claim 1, wherein the transaction is a commercial transaction involving a credit card number.
7. The method of claim 1, wherein the request sent to the user is in a form of an applet requesting personal information about the user.
8. A method in a data processing system for managing information, the method comprising:
 - \sending a Web page to a user at a client;
 - receiving a response, wherein the response include the information;
 - processing a business transaction with the client using the information;
 - storing the information to form stored information;
 - receiving a request to remove the stored information; and
 - removing the stored information in response to receiving the request.
9. The method of claim 8, wherein the request is received after retaining the stored information is unnecessary to the business transaction.
10. The method of claim 8, wherein the business transaction is a purchase of an item using a credit card.

11. A distributed data processing system comprising:

a network;

a plurality of clients connected to the network; and

a server connected to the network, wherein the server receives information from the plurality of clients in which the information is received in association with serving Web pages and receiving the information in response to serving the Web pages, stores the information to form stored information, receives a request from a client within the plurality of clients to discard a portion of the information from the stored information, removing the portions of the information from the stored information in response to receiving the request.

12. A data processing system comprising:

a bus system;

a communications unit connected to the bus system;

a memory connected to the bus system, wherein the memory includes a set of instructions; and

a processing unit connected to the bus system, wherein the processing unit executes the set of instructions to receive information from a plurality of users; store the information to form stored information; receive a request to remove selected information from the stored information from a user within the set of users, wherein the selected information is received in response to a transaction involving the user; and remove the selected information from the stored information in response to receiving the request.

13. A data processing system comprising:

a bus system;

a communications unit connected to the bus system;

a memory connected to the bus system, wherein the memory includes a set of instructions; and

a processing unit connected to the bus system, wherein the processing unit executes the set of instructions to send a Web page to a user at a client; receive a response, wherein the response include the information; process a business transaction with the client using the information; store the information to form stored information; receive a request to remove the stored information; and remove the stored information in response to receiving the request.

14. A data processing system for managing information, the data processing system comprising:

first receiving means for receiving information from a plurality of users;

storing means for storing the information to form stored information;

second receiving means for receiving a request to remove selected information from the stored information from a user within the set of users, wherein the selected information is received in response to a transaction involving the user; and

removing means for responsive to receiving the request, removing the selected information from the stored information.

15. The data processing system of claim 14, wherein the second receiving means includes:

means for determining whether the request is a valid request; and

means for preventing removing of the selected information in response to a determination that the request is an invalid request.

16. The data processing system of claim 14, wherein at least one of a certificate, a password, and a key is used to determine whether the request is valid.

17. The data processing system of claim 14, wherein the selected information is personal information about the user.

18. The data processing system of claim 17, wherein the personal information includes at least one of a user name, a user identification, a password, a telephone number, an e-mail address, a physical address, a social security number, a birth date, and a credit card number.

19. The data processing system of claim 14, wherein the transaction is a commercial transaction involving a credit card number.

20. The data processing system of claim 14, wherein the request sent to the user is in a form of an applet requesting personal information about the user.

21. A data processing system for managing information, the data processing system comprising:

sending means for sending a Web page to a user at a client;

first receiving means for receiving a response, wherein the response include the information;

processing means for processing a business transaction with the client using the information;

storing means for storing the information to form stored information;

second receiving means for receiving a request to remove the stored information; and

removing means for removing the stored information in response to receiving the request.

22. The method of claim 21, wherein the request is received after retaining the stored information is unnecessary to the business transaction.

23. The data processing system of claim 21, wherein the business transaction is a purchase of an item using a credit card.

24. A computer program product in a computer readable medium for managing information, the computer program product comprising:

first instructions for receiving information from a plurality of users;

second instructions for storing the information to form stored information;

third instructions for receiving a request to remove selected information from the stored information from a user within the set of users, wherein the selected information is received in response to a transaction involving the user; and

fourth instructions, responsive to receiving the request, for removing the selected information from the stored information.

25. A computer program product in a computer readable medium for managing information, the computer program product comprising:

first instructions for sending a Web page to a user at a client;

second instructions for receiving a response, wherein the response include the information;

third instructions for processing a business transaction with the client using the information;

fourth instructions for storing the information to form stored information;

fifth instructions for receiving a request to remove the stored information; and

sixth instructions for removing the stored information in response to receiving the request.

26. The method of claim 25, wherein the request is received after retaining the stored the information is unnecessary to the business transaction.

27. The method of claim 1, wherein the request to remove selected information originates from a client device of the user.

28. The method of claim 1, wherein the stored information is information stored on a server.

29. The method of claim 8, wherein the request to remove stored information originates from a client device of the user.

30. The method of claim 8, wherein the stored information is information stored on a server.
31. The method of claim 14, wherein the request to remove selected information originates from a client device of the user.
32. The method of claim 14, wherein the stored information is information stored on a server.
33. The method of claim 21, wherein the request to remove stored information originates from a client device of the user.
34. The method of claim 21, wherein the stored information is information stored on a server.